DETAILED ACTION

In view of **Appeal Brief** filed on 13 May 2009 and an authorization for this Examiner's Amendment given in a telephone interview with Brian N. Fletcher on 27 July 2009, the claimed subject matters are thus distinctly pointed out as patentable features to place the application in the condition for allowance.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Brian N. Fletcher (Reg. No. 51,683) on 27 July 2009.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 3.

Replace claim 1 and 4 as follows.

Claim 1:

A cryptographic method, ~~during which an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less~~

~~than or equal to m and bn-1 is non-zero, bn-1 being the most significant bit of the number b,~~ comprising the steps of:

performing an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b by a processor, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_n-1 is non-zero, b_n-1 being the most significant bit of the number b;

masking the number a by a random number p by the processor before performing the integer division and/or the modular reduction[[,]];

taking away the contribution made by the random number p from the result of the integer division after having performed the integer division; and

generating encrypted or decrypted data by the processor in accordance with a result of the division and/or modular reduction.

CANCEL CLAIM 3

CLAIM 4:

A method according to claim [[3]]1, wherein …

Allowable Subject Matter

Claims 1, 2 and 4 – 8 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 1 (& associated dependent claims).

The present invention is directed to a method of performing an integer division of a type q = a div b and/or a modular reduction of a type r = a mod b by a processor, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_n-1 is non-zero, b_n-1 being the most significant bit of the number b. No singular art disclosing, nor motivation to combine has been found to anticipate or render obvious the claimed invention of masking the number a by a random number p by the processor before performing the integer division and/or the modular reduction; taking away the contribution made by the random number p from the result of the integer division after having performed the integer division; and generating encrypted or decrypted data by the processor in accordance with a result of the division and/or modular reduction.

.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Patent Examiner
Art Unit 2431
7/28/2009